Defense Information Systems Agency

A Combat Support Agency

Secure Configuration Management (SCM) and Continuous Monitoring Overview

David Hoon
DISA PEO-MA
SCM PMO Lead

16 AUGUST2011

DISA
A Combat Support Agency

SCM Agenda

- **What is SCM?**
- **Why SCM?**
- **Gap Analysis**
- **SCM Initiatives**
  - Management of Assets & Inventory
  - Compliance Checking & Reporting of Assets
  - Continuous Monitoring of Assets
  - Patch the GIG
- **SCM Roadmap**
- **SCM Support for Continuous Monitoring**
- **DISA Testing**

DISA
A Combat Support Agency

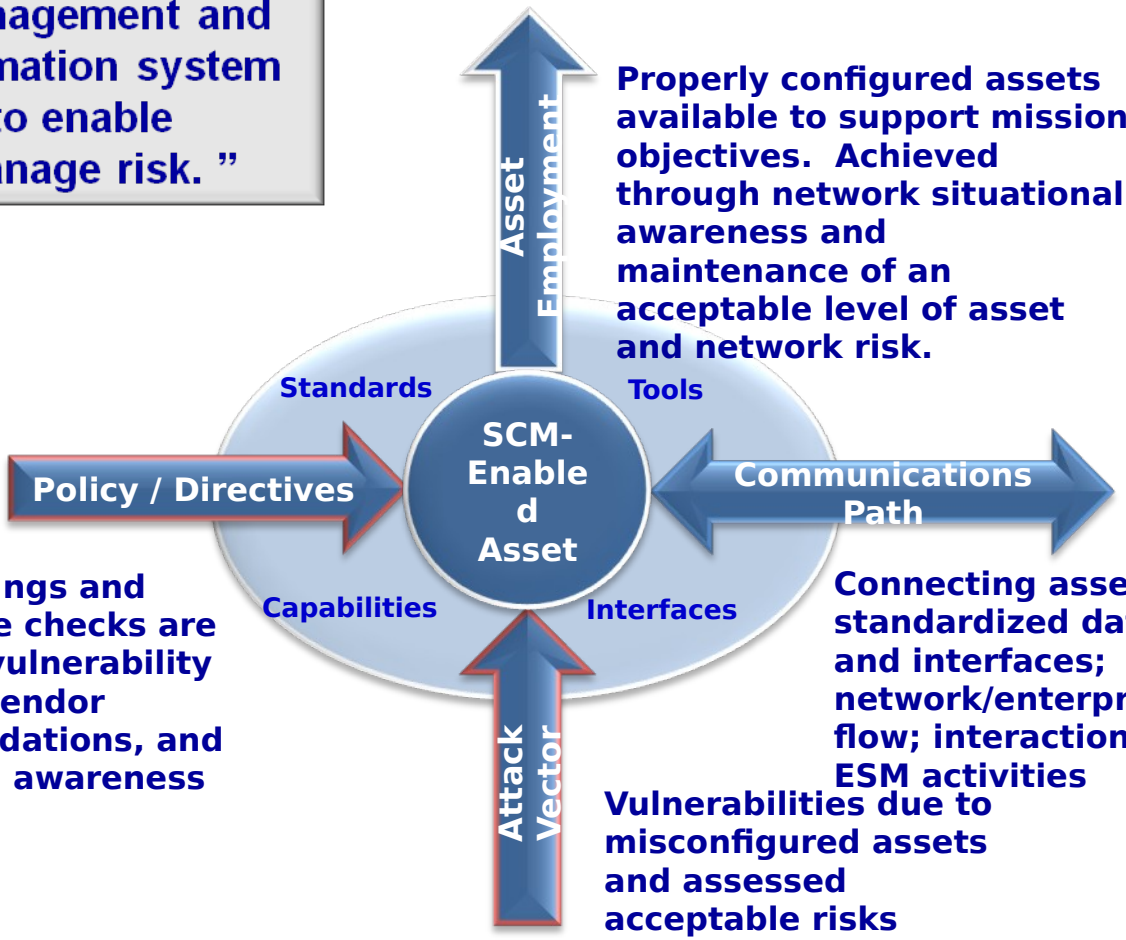
What is SCM?

- **SCM is the integration and optimization of enterprise IA applications, tools, and data standards to support automated processes for risk management.**
  - **SCM delivers capabilities to provide enterprise awareness of DoD asset inventory and enterprise vulnerability exposures and enables valued business processes**
- **Simply put, SCM is:**
  - **Configuring assets securely in the first place**
  - **Maintaining secure configuration**
  - **Providing continuous situational awareness to the right people**

DISA
A Combat Support Agency

The SCM Paradigm

SCM: "The management and control of information system configurations to enable security and manage risk."



Properly configured assets available to support mission objectives. Achieved through network situational awareness and maintenance of an acceptable level of asset and network risk.

Asset settings and compliance checks are based on vulnerability analysis, vendor recommendations, and situational awareness

Connecting assets via standardized data formats and interfaces; network/enterprise data flow; interaction with other ESM activities

Vulnerabilities due to misconfigured assets and assessed acceptable risks

DISA
A Combat Support Agency

The SCM Paradigm

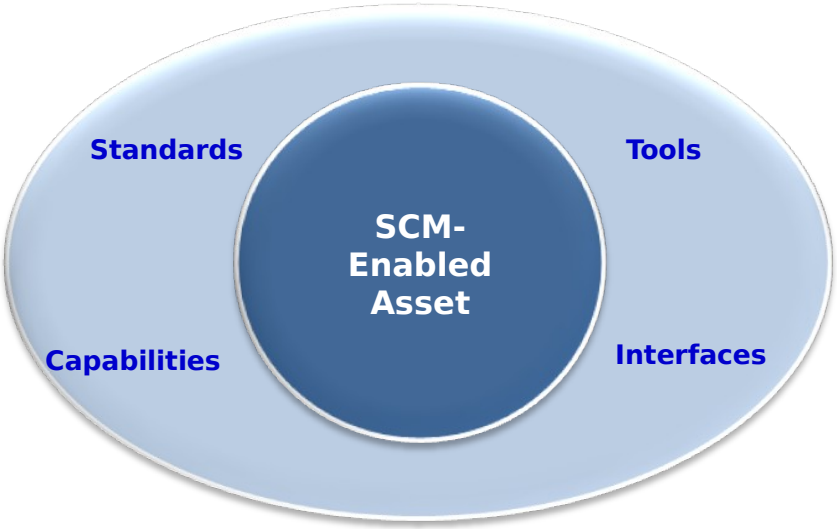
The SCM Program implements published standards, using validated tools and employs standardized interfaces to realize essential Secure Configuration capabilities.

Standards: Secure Configuration Automation Protocol (SCAP). A NIST-developed, industry-adopted set of standards supporting interoperability and automated data exchange. Extended to include standard data formats for reporting asset and summary information.

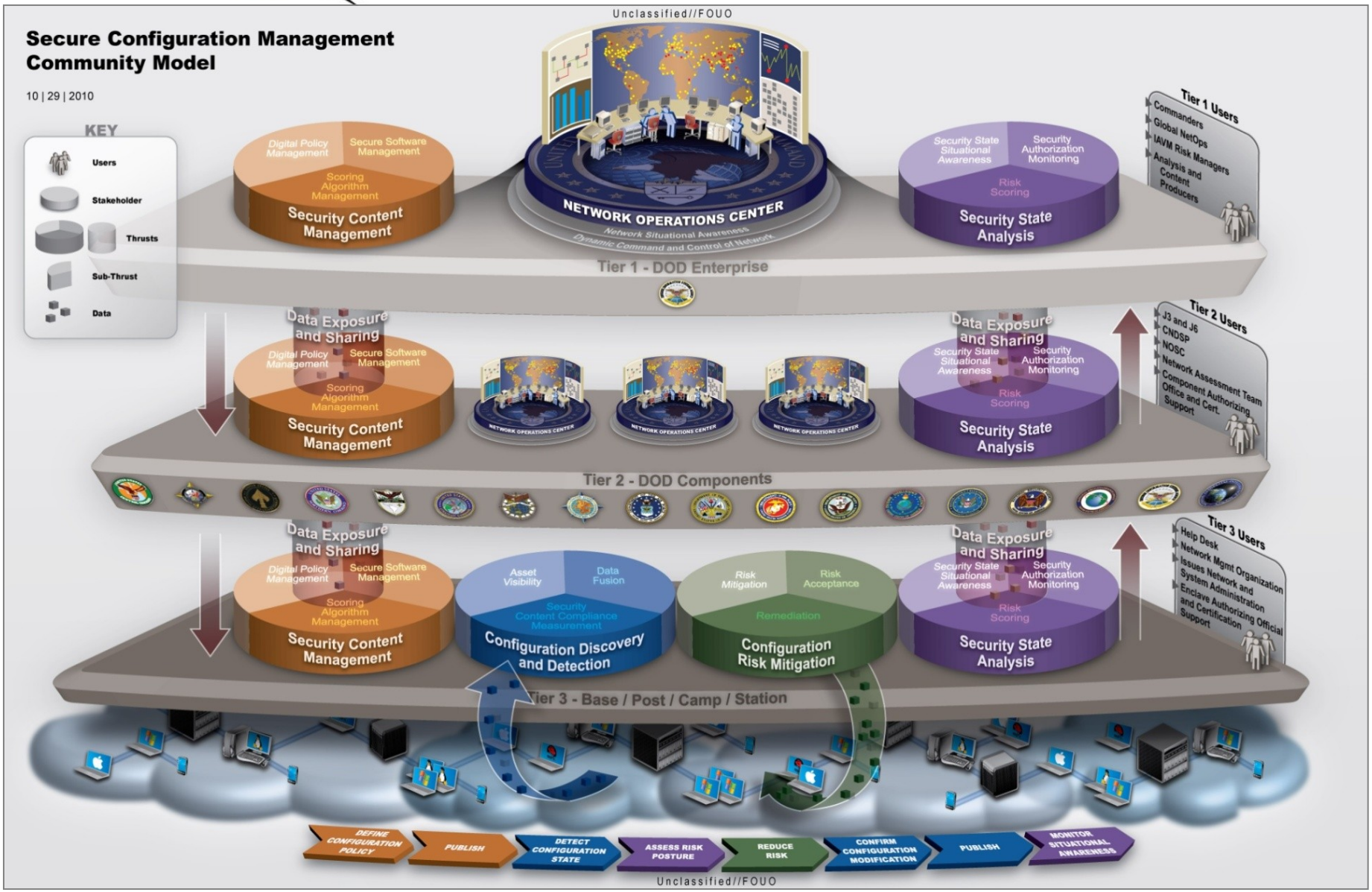
Tools: Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) tools validated as conforming to SCAP standards.

Interfaces: Leverage SCAP and emerging standards (Asset Report Format (ARF) / ARF Summary Report (ASR)) to distribute asset data by defining data input and output formats for SCAP-validated tools

Capabilities: Content/Policy development; Asset Inventory/Discovery; Security State Analysis/Risk Assessment; and Risk Mitigation



SCM Community Model

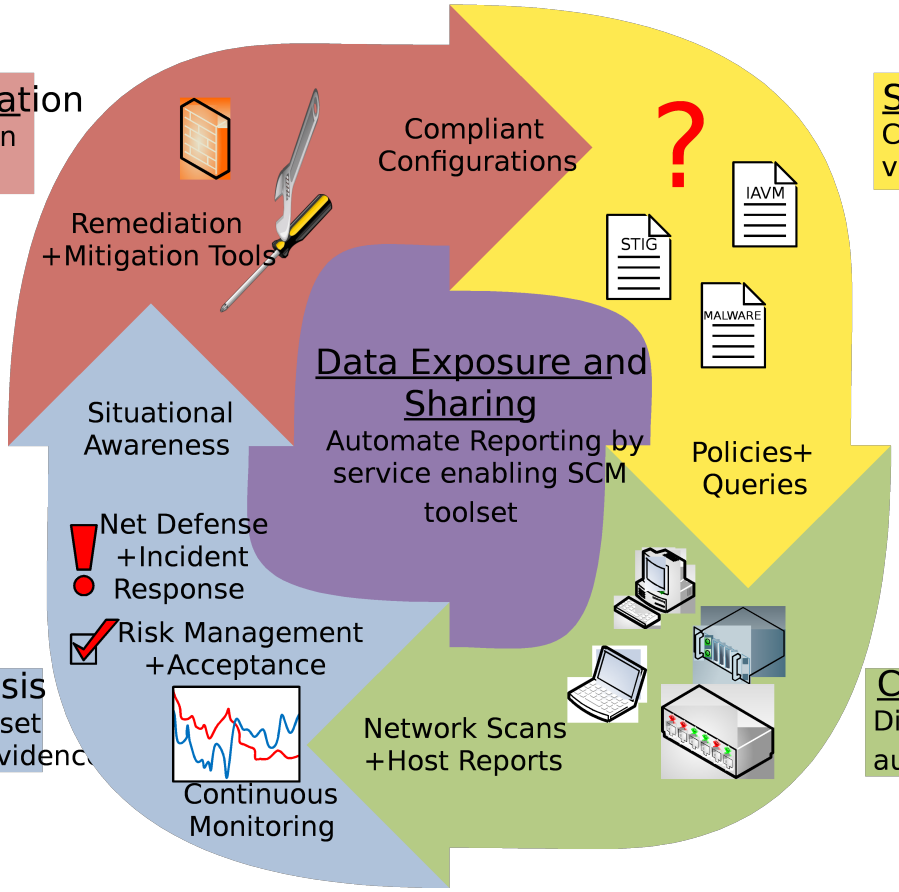


DISA
A Combat Support Agency

SCM Lifecycle

Configuration Risk Mitigation
Allow for the remediation of non secure configurations

Security Content Management
Create and distribute content for vulnerability and configuration tools



Security State Analysis
Assess risk by correlating asset attributes and compliance evidenc

Configuration Discovery and Detec
Discover and audit assets with standardized automated tools

DISA
A Combat Support Agency

Why SCM?
Today's Solutions Do Not Work

The Enterprise Today:

- **Difficult to maintain secure configurations: high level of effort, low return on investment**
- **Disparate IA tool sets: proprietary capabilities, disconnected and stand-alone configurations**
- **Manual reporting: resource intensive, slow, inaccurate**
- **Lack of situational awareness: data and configuration control silos, can't organize data by COCOM, Service, or mission**
- **Inconsistent standards: vulnerability risk**

DISA

A Combat Support Agency

Gap Analysis

Goals and Benefits	Processes to Improve	SCM Initiatives
Interoperability Leverage DoD Investment	**ASSET TRACKING** •Manual, inconsistent, labor intensive **ASSET SCANNING** •SCCVI •FSO Developed Scripts	Management of Assets & Inventory
Alleviate Operator Pain	**POA&M** •Manual, labor intensive, questionable **REPORTING TO VMS** •Manual, difficult to use, questionable	Compliance Checking & Reporting of Assets
Manpower Savings	**CYBER COMMAND READINESS INSPECTION (CCRI)** •Manual, partial check, labor intensive **CERTIFICATION AND ACCREDITATION (C&A)** •Manual, duplicative, labor intensive	Continuous Monitoring of Assets
Improve Security Posture	**INFORMATION ASSURANCE VULNERABILITY MANAGEMENT - IAVM** •Manual, inconsistent, unknown **PATCHING** •Manual, labor intensive, inconsistent	Patch the GIG

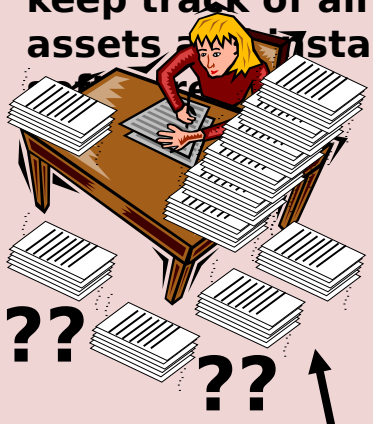
SCM Initiatives

1. Management of Assets & Inventory
2. Compliance Checking & Reporting of Assets
3. Continuous Monitoring of Assets
4. Patch the GIG

Management of Assets & Inventory

A Combat Support Agency

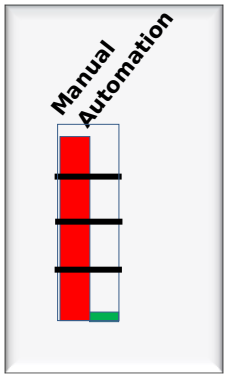
1 System Administrator is forced to manually keep track of all assets and installed



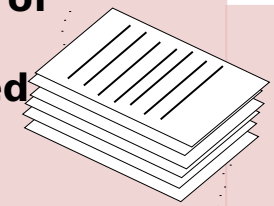
??

??

??



2 Inventory of devices is maintained manually and configuration changes are not consistently documented



3 Standard device information like operating system, software installed, and other settings may or may not be manually collected

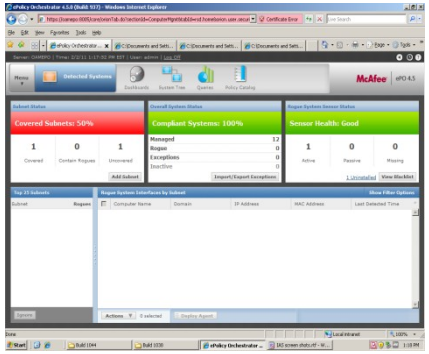
4 No standard reporting

Situational Awareness ??

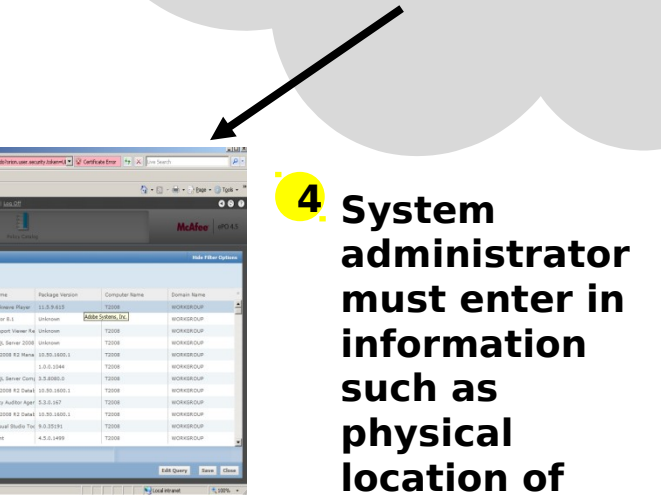
SCM Initiative: Management of Assets &Inventory

DISA
A Combat Support Agency

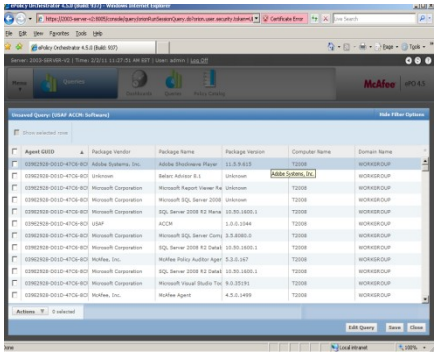
1. Network devices are discovered using automated means



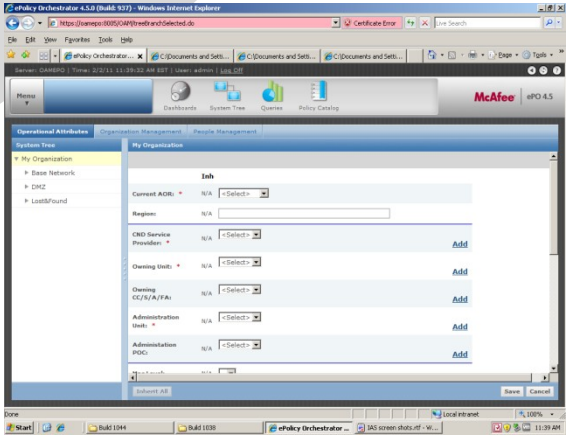
2. Agents are automatically deployed to all devices on network

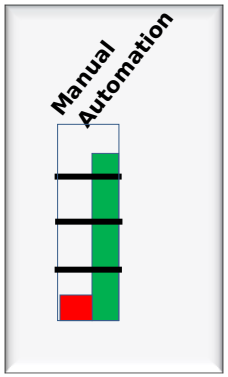


3. Agents gather information about the assets (e.g. installed sw, version information, etc.) on the network and



4. System administrator must enter in information such as physical location of box ,etc.





Network Situational Awareness

Compliance Checking of Assets

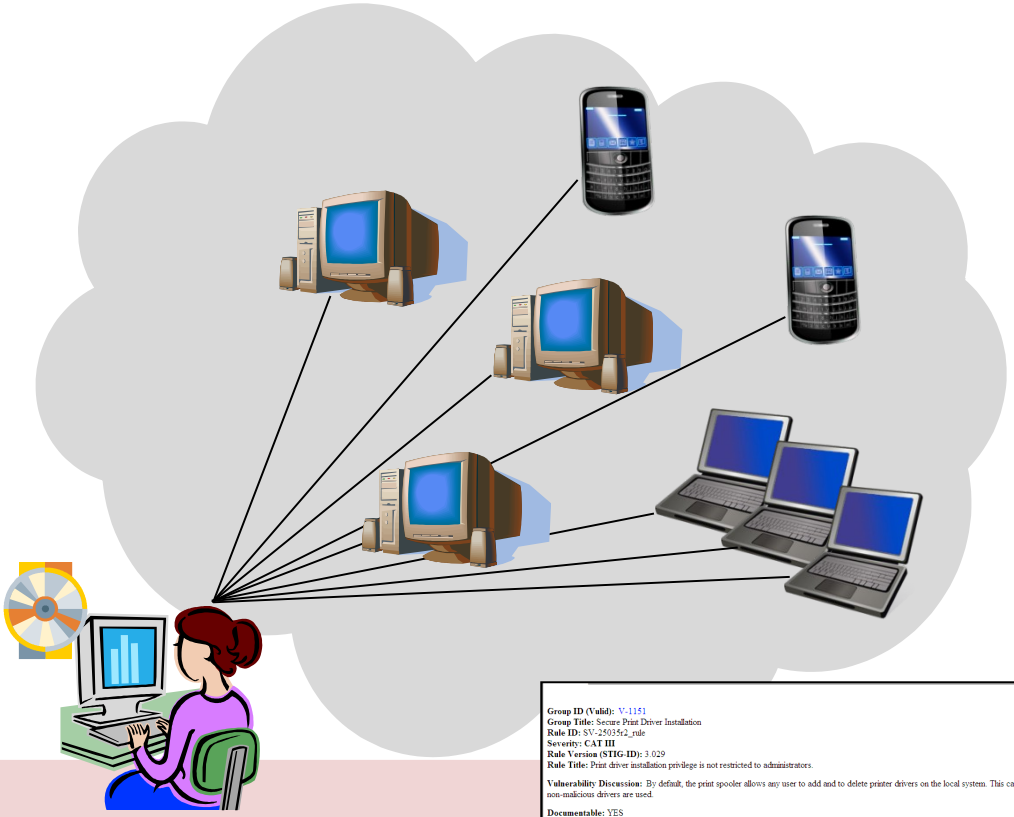
A Combat Support Agency

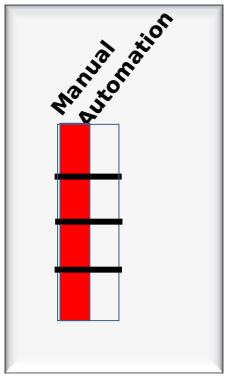
1. Policy created dictates Security Technical Implementation Guides (STIGs)

Policy
Policy
Policy

2. STIGs are written and maintained by DISA Field Support

3. System Administrator must manually download STIGs or rely on interim fixes like Gold Disk to





4. System Administrators need to manually check settings (there are 261 checks in the latest version of Windows 7 STIG) FOR EACH Asset

Group ID (Vulid): V-1151
Group Title: Secure Print Driver Installation
Rule ID: SV-25035r2_rule
Severity: CAT III
Rule Version (STIG-ID): 3.029
Rule Title: Print driver installation privilege is not restricted to administrators.

Vulnerability Discussion: By default, the print spooler allows any user to add and to delete printer drivers on the local system. This capability should be restricted to privileged groups to ensure only stable, non-malicious drivers are used.

Documentable: YES
Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options.

If the value for "Devices: Prevent users from installing printer drivers" is not set to "Enabled", then this is a finding.

The policy referenced configures the following registry value:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers

Value Name: AddPrinterDrivers

Value Type: REG_DWORD
Value: 1

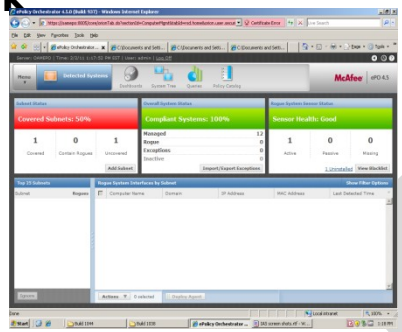
Documentable Explanation: If site circumstances require that users be able to install print drivers for locally attached printers (e.g. - Users that telecommute and attach a home printer), this exception can be documented with the site IAO.

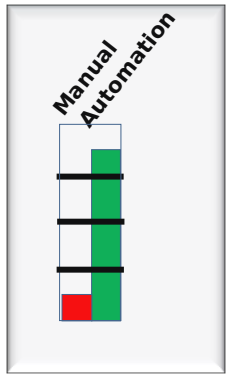
Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Devices: Prevent users from installing printer drivers" to "Enabled".

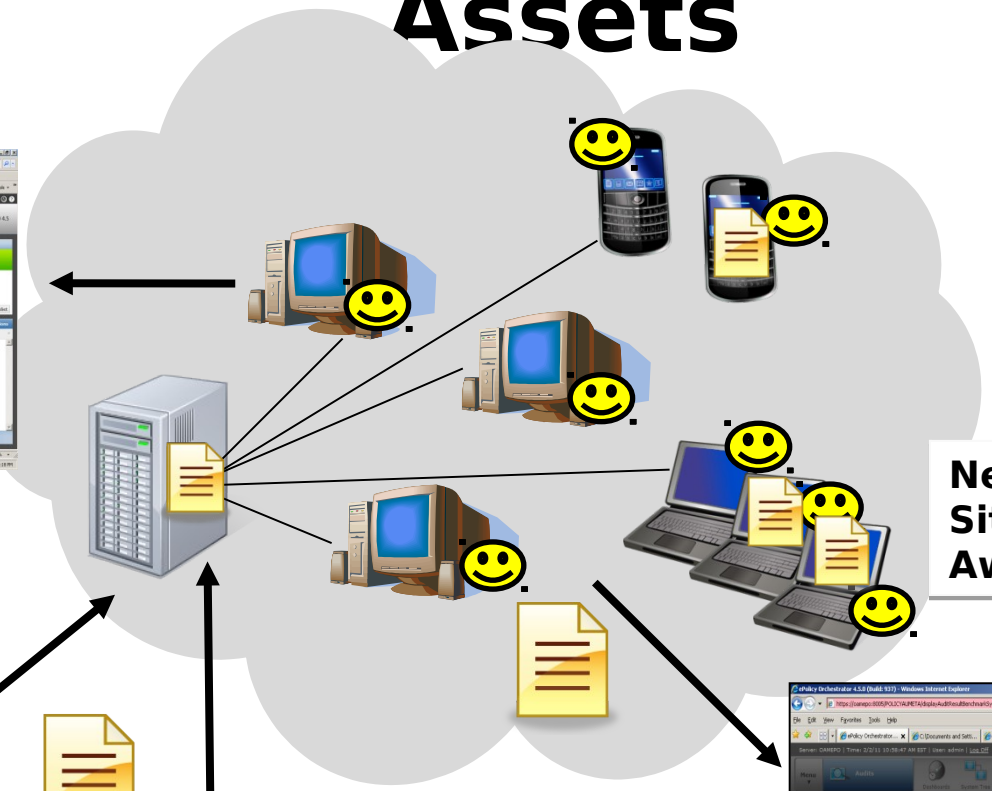
SCM Initiative: Compliance Checking of Assets

A Combat Support Agency

1. **Agents exist on managed assets on network**

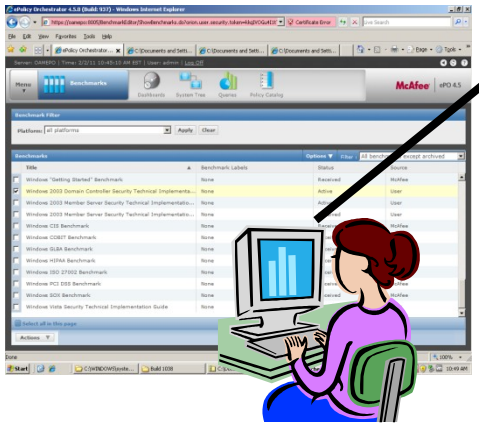


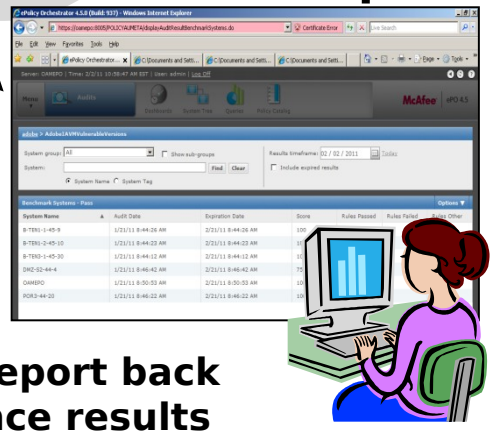




2. **Compliance checking can be managed from one central place FOR ALL NETWORK assets**

Network Situational Awareness





Authority

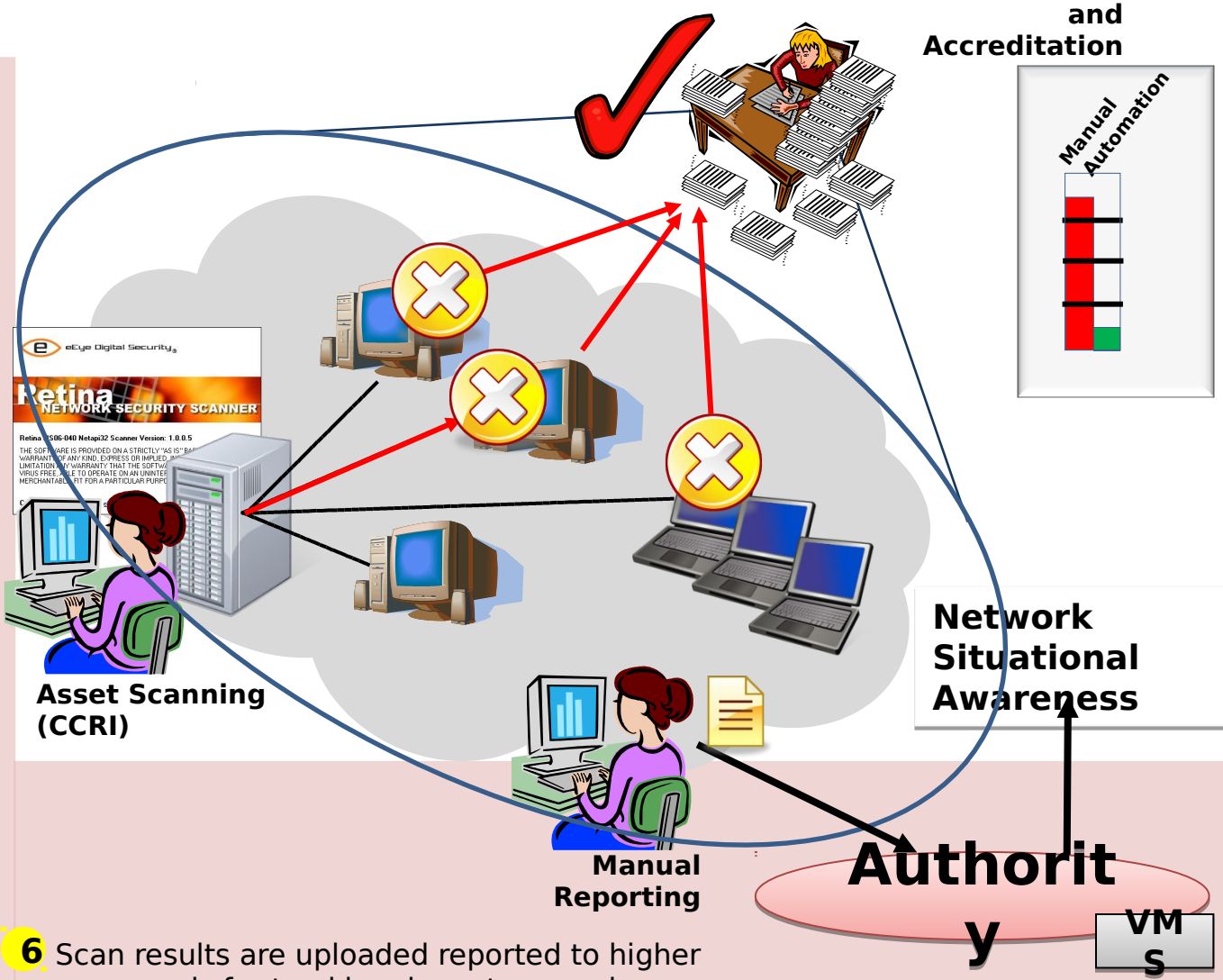
3. **Agents downloads compliance check information in standardized (SCAP) format**

4. **Agents report back compliance results continuously**

Monitoring of Assets

A Combat Support Agency

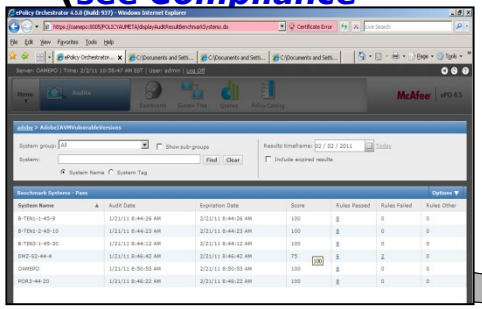
1. Initially each network/system goes through a Certification and Accreditation (C&A) process. This is a very labor intensive process and done about every 3 years.
2. Once assets go through C&A, asset changes require manual updates to original C&A documentation.
3. Periodic evaluations of the configurations of the boxes takes place during Command Cyber Readiness Inspections (CCRI). This is very labor intensive and may involve weeks of preparation by network admin consists of a series of manual checks and a asset scans using SCCVI (eEye Retina).
4. CCRI consists of
5. Based on the results from the network scans changes are made to the assets . Updates to C&A documentation may be required.
6. Scan results are uploaded reported to higher commands for tracking ,inventory, and Situational Awareness purposes. In some cases a great deal of manual reporting is required into Vulnerability Management System (VMS)

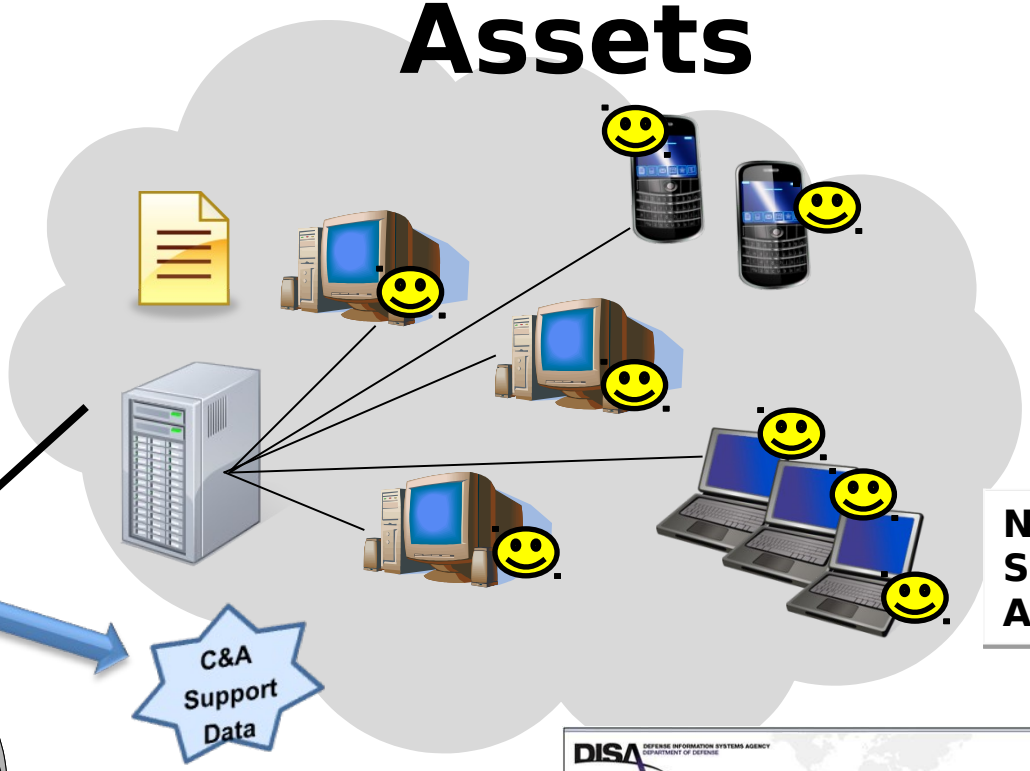


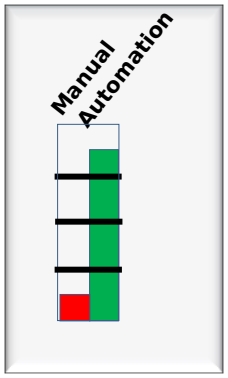
SCM Initiative : Continuous Monitoring of Assets

DISA
A Combat Support Agency

1. **Compliance results and metrics are continuously reported and made available to the C&A process (see *Compliance*)**

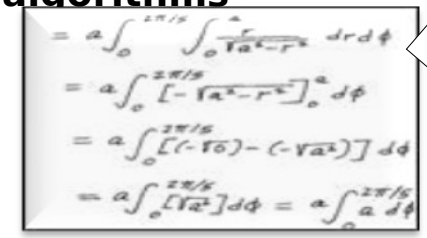




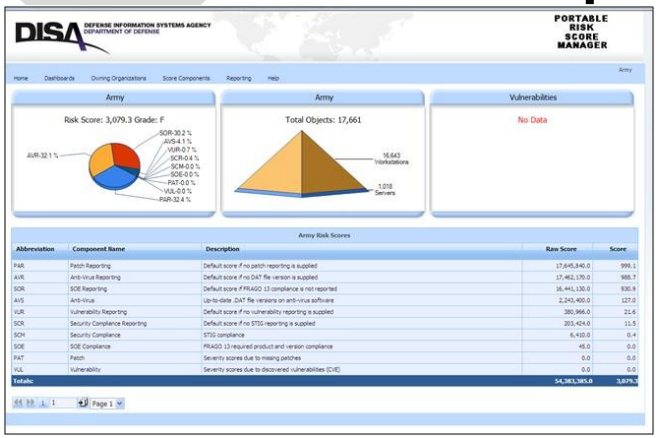


Network Situational Awareness

2. **Results and metrics are used as inputs to Scoring algorithms**



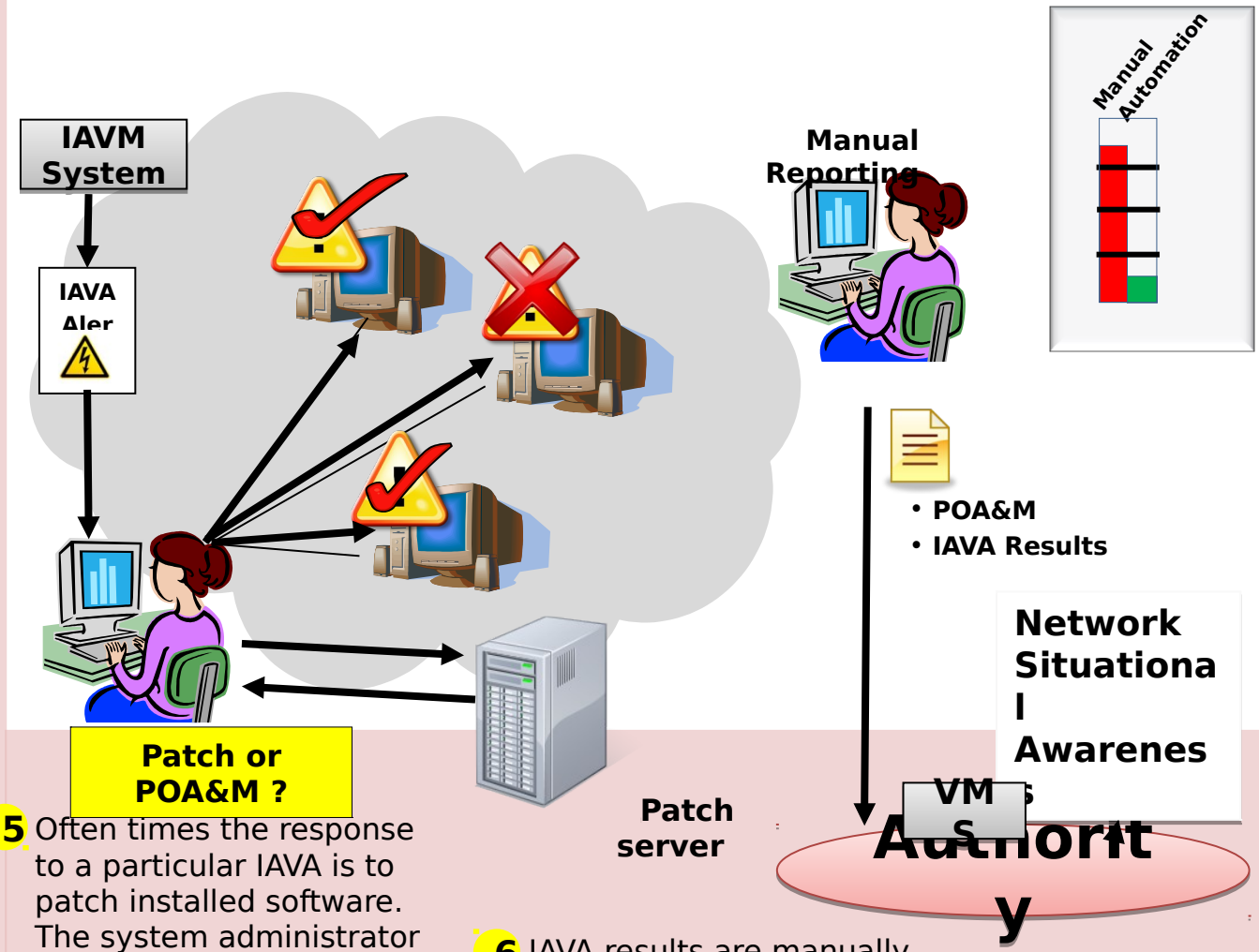
3. **Scoring algorithms are used to perform risk assessment and determine risk score for assets on network**



“Patch The GIG”

A Combat Support Agency

1. Policy dictates an Information Assurance Vulnerability Alert (IAVA) mandating updates to the configuration of an asset.
2. The IAVAs are distributed to system administrators as they become available dictating fixes that need to be made to systems based on newly identified vulnerabilities
3. The system administrator has the responsibility of checking to see which IAVAs are relevant the systems that are being managed.
4. The system administrator must patch the systems or make desired configuration changes as per the IAVA or come up with a plan of when the desired changes will be made called a Plan Of Action & Milestones (POA&M)



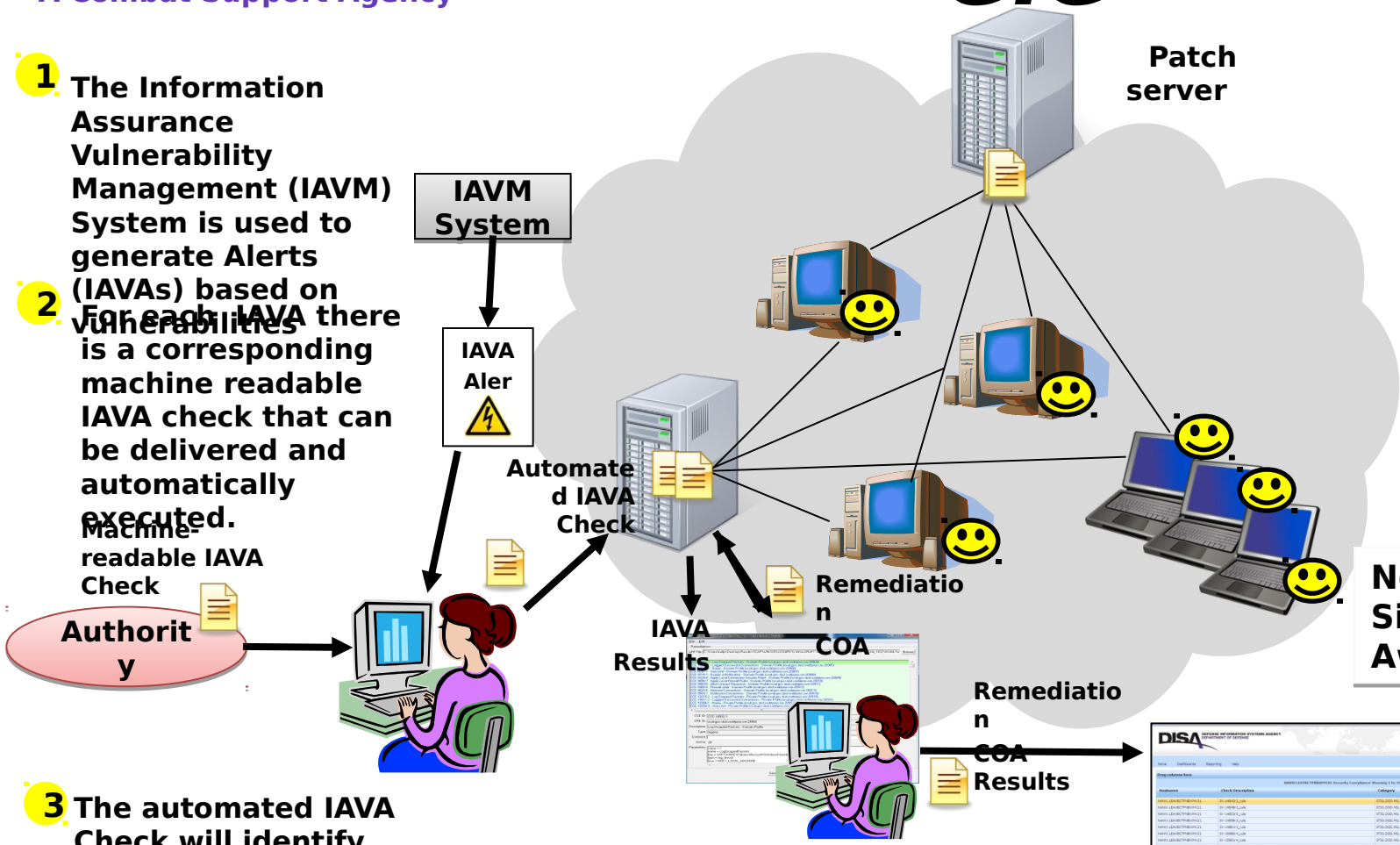
5. Often times the response to a particular IAVA is to patch installed software. The system administrator must download and install patch information from the patch server.
6. IAVA results are manually reported into VMS

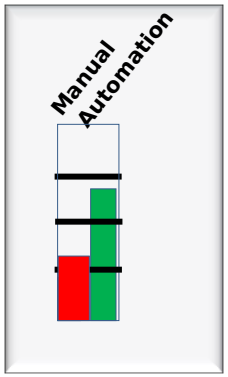
SCM Initiative : Patch the GIG

A Combat Support Agency

1. The Information Assurance Vulnerability Management (IAVM) System is used to generate Alerts (IAVAs) based on vulnerabilities

2. For each IAVA there is a corresponding machine readable IAVA check that can be delivered and automatically executed.





3. The automated IAVA Check will identify systems to which the IAVM applies

4. The results will be used to make a Remediation Course of Action decision (patch, fix, mitigate,

Remediation Course of Action Determination

5. The Remediation Course of Action is conducted and results are automatically reported.

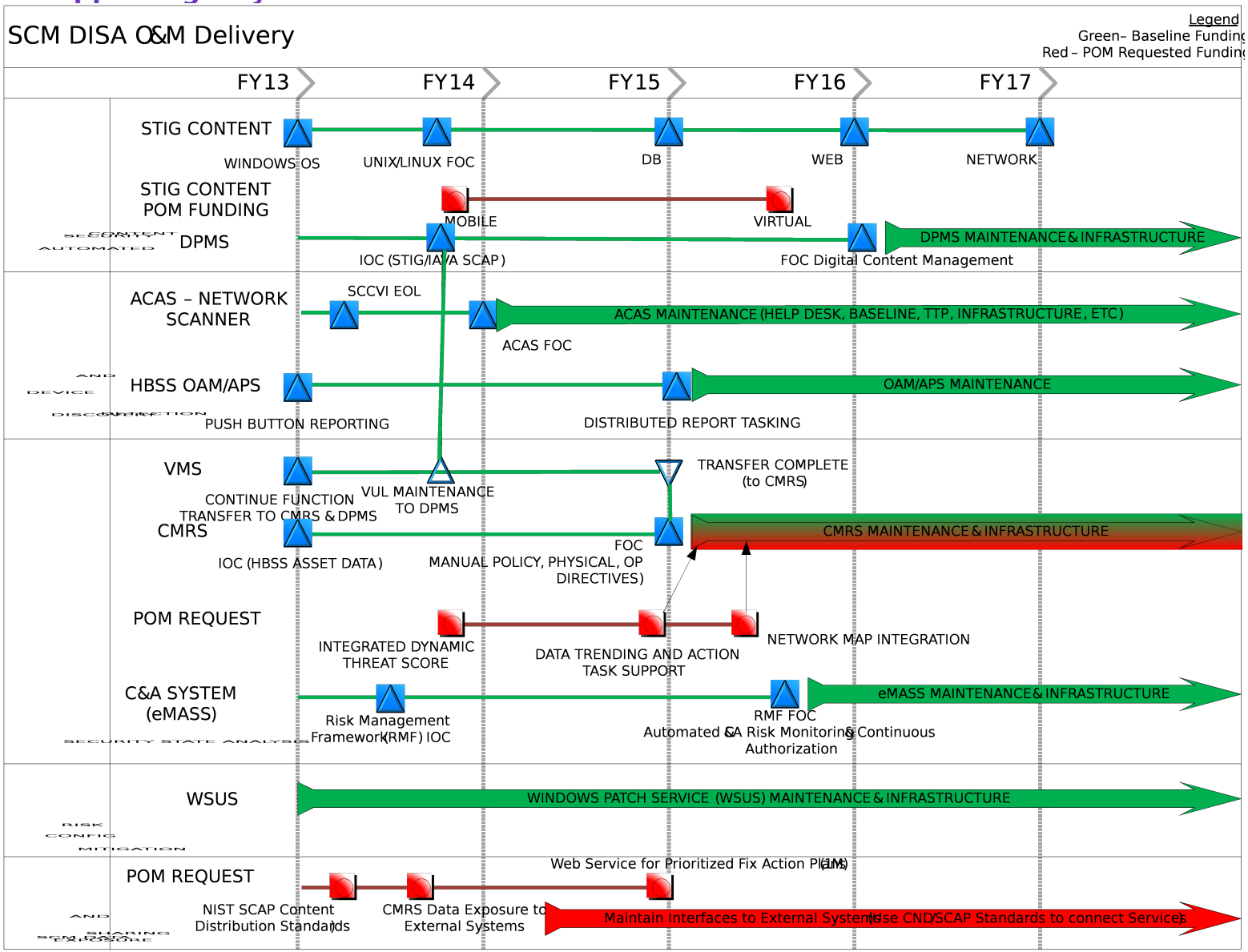
Secure Configuration Management Capabilities

DISA
A Combat Support Agency

SCM Capabilities & Goals	Current	Near Term (FY11-12)	Long Term (FY13…17)
Continuous Monitoring	Manual reporting and tracking, snapshot in time, inaccurate, slow	•Standards-based network scanner •Windows System software inventory •Automated SCAP policy distribution to HBSS •Continuous Monitoring IOC (e.g., STIG, IAVM, Patch, AV, FRAGO 13 compliance)	•Integrated standards and tools for automated reporting of non-automated compliance checks (e.g., Q&A policy checks using OCIL) •Automated SCAP policy distribution to SCAP tools •Non-windows system software and mobile device inventory
Compliance Inspections (e.g., CCRI)	Automated review tools, manual follow up data entry and reporting	•Use SCCVI imports for CCRI after action compliance reporting •Integrate HBSS compliance data	•Mission readiness views •Integrate standard-s based security assessment content, tools, and reporting (e.g., ACAS, SCCM)
Automate Certification and Accreditation	A manual and labor intensive process that provides snapshots of the security risks that systems and enclaves over a 3 year period	•Automate Windows STIG and IAVM assessment content •Implement continuous reporting and risk scoring •Test POAM reduction •Test Risk Management Framework (RMF)	•Automate residual risk awareness using CCIs •Continuous Authorization using RMF •Security State Change awareness •Automate non-windows system software and mobile device inventory
“Patch the GIG”	IAVM process, manual assessments	•Support operational test of remediation standards	•Deploy automated, integrated remediation language to speed up transmission of critical fix/remediation actions (does not automatically fix,

SCM Schedule FY13-17

A Combat Support Agency



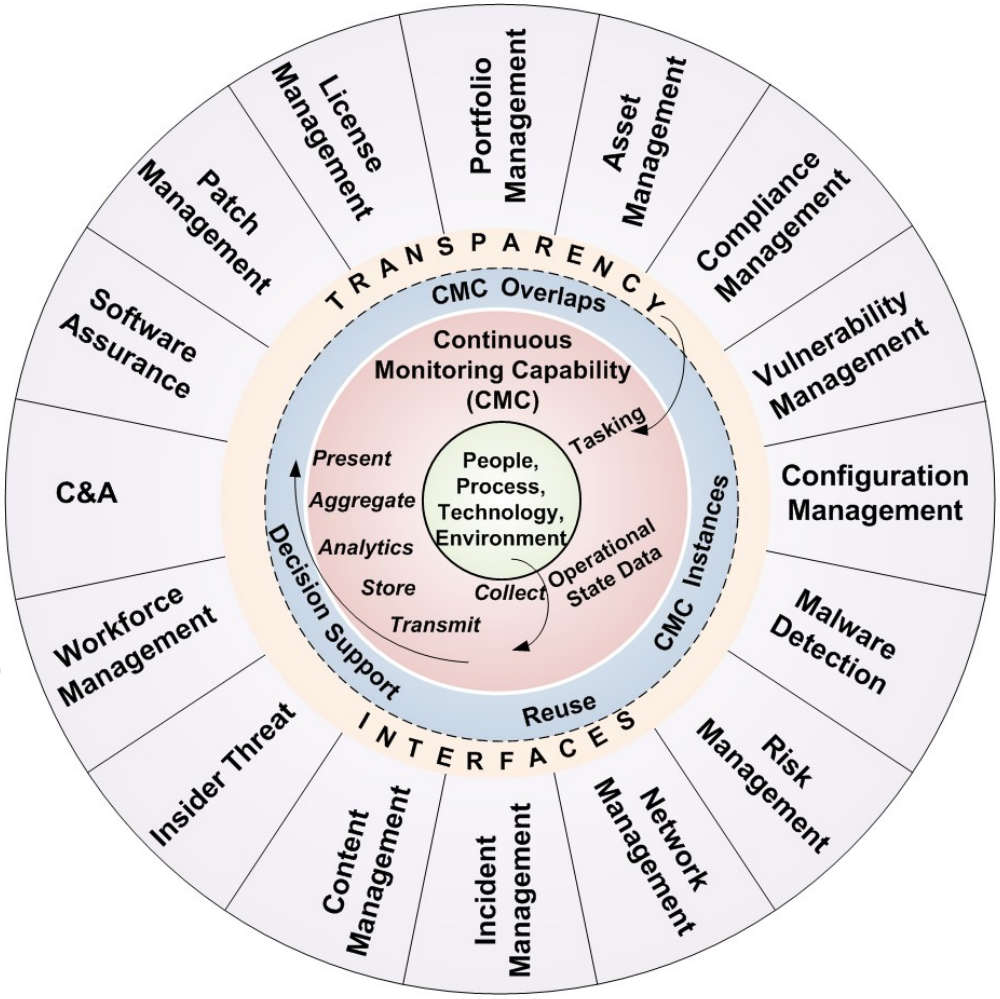
Continuous Monitoring Capability (CMC) in DoD

A Combat Support Agency

- **Continuous Monitoring:**
  Maintaining ongoing awareness to support organizational risk decisions.

- **CMC unifies existing disparate capabilities of operational management and control to build out a robust, automated and integrated solution for expedited decision processes of all aspects of future computer network operations.**

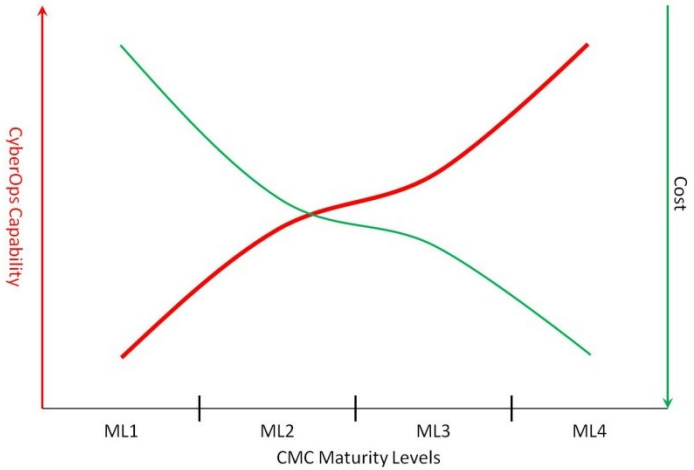
- **Executed through a Maturity Level Concept**



drivers of CM: Presidential, Legislative, and DoD Efficiency

A Combat Support Agency

CMC Maturity Levels (ML)



ML1: Windows, Non-Windows, and Network Asset Visibility with Vulnerability, Security Configuration, and Patch compliance status

ML2: Common Enterprise Risk Scoring; Integrated Host and Network Scan data; Publish analysis results to CC/S/A/FA; CAG Compliance

ML3: Integration with CNDSP Operations; Continuous Authorization (C&A Automated); Integrate with RED/Blue Team efforts

ML4: Dynamic Threat Integration; Mission Focused Risk Assessments; Integrated Remediation Management

BLUF: Increasing automation reduces manual efforts and permits resource recovery

DISA

A Combat Support Agency

DISA PILOTING

DISA
A Combat Support Agency

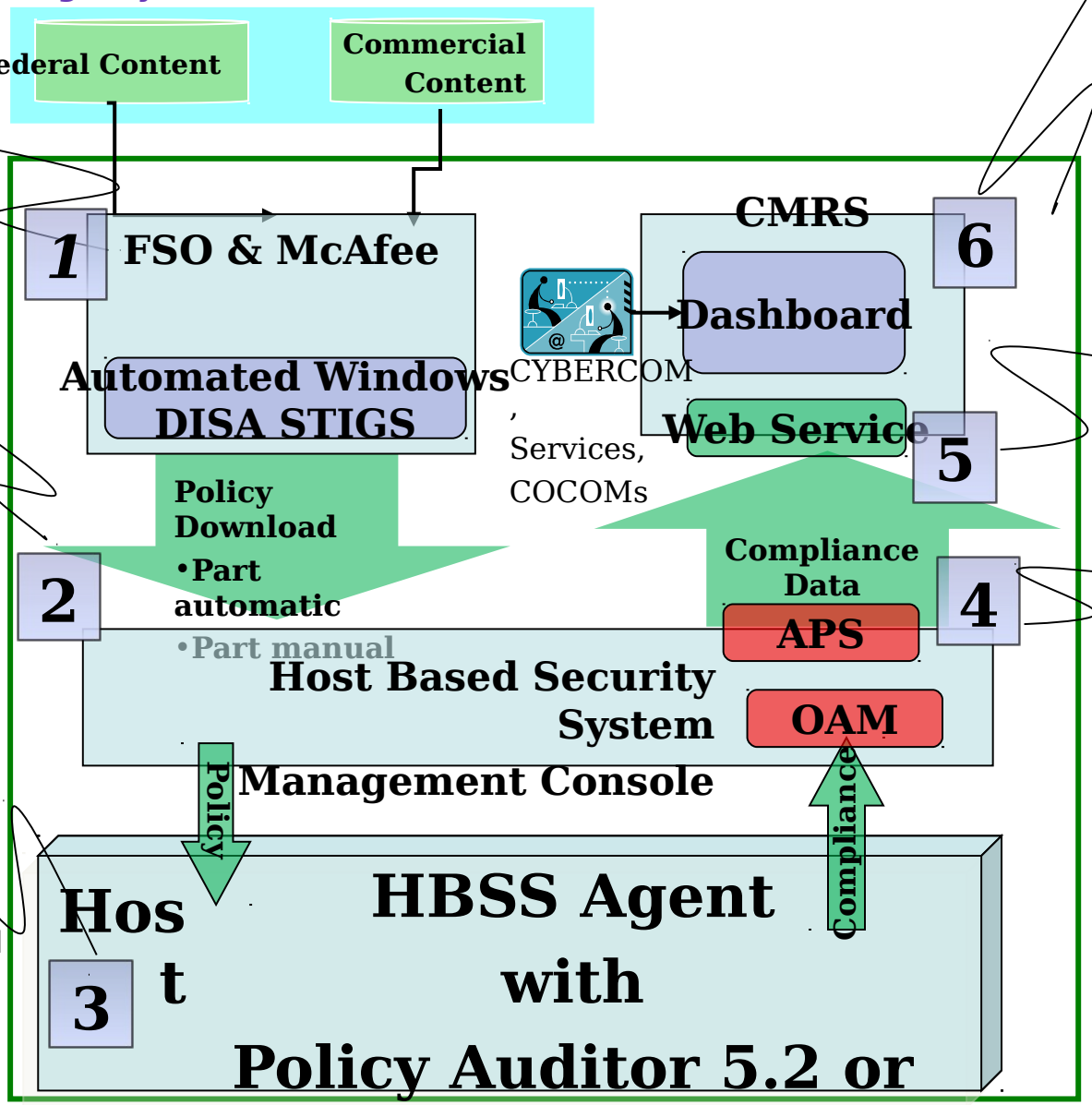
DISA Operational Testing

- Continuous Monitoring Risk Scoring (CMRS) Objectives:
  - Increase visibility of cyber risks
  - Implement integrated automated and continuous operations of security tools
  - Produce a consistent, understood picture of enterprise & component risk posture
- CMRS supports the following four primary use cases:
  - ***Certification and Accreditation Automation:*** FSO is responsible for integrating HBSS continuous monitoring capabilities into C&A process and tools, transform from current C&A process to continuous authorization process
  - ***IAVM Reporting:*** CIO is responsible for eliminating singular, manually-entered POA&Ms, utilize automated capabilities to report IAVM compliance to USCYBERCOM, evolve IAVM reporting based on vulnerability exposures, threats, and impacts
  - ***CCRI Automation:*** FSO is responsible for automation with VMS to minimize manual data entry, and develop a way forward to use HBSS and ACAS to support CCRI leveraging continuous monitoring
  - ***Improved NetOps:*** DCC is responsible for leveraging existing HBSS continuous monitoring capabilities to target Ops countermeasures based on current threat intelligence and attack vectors

UNCLASSIFIED

Deployed SCM Framework

A Combat Support Agency



1.DISA STIGs auto-distributed using HBSS Architecture

2. STIG, and IAVM (future) Content is imported into HBSS

3. The HBSS Policy Auditor checks host compliance and reports results to the HBSS Console

6. The continuous monitoring application applies threat-based scoring algorithms to create risk views by COCOM, CC/S/A/FA, or global picture

5. A web service consumer receives machine-to-machine data from HBSS and writes to the data repository.

4a. HBSS uses OAM to tag devices with owner, AOR, and CNDSP
4b. HBSS uses APS to publish data to the Continuous Monitoring Application.

Existing & deployed

Existing not fully deployed

UNCLASSIFIED

A Combat Support Agency

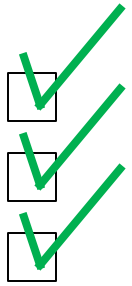
Rollout Status

Done

- Deploy & configure Operational Attribute Module (OAM)
- Deploy Asset Publishing Service (APS)
- Run Operating System STIGs to report security status

To Do

- Run IAVM compliance checks to report IAVM compliance
- Deploy Asset Configuration Compliance Module (ACCM)
- Update CM/RS beta to address CIO, FSO, and DCC requirements
- Negotiate w/US Cyber to accept IAVM reporting using automated displays in CMRS
- Transition annual re-accreditation to CMRS-based risk decision
- Use automated reports to close out CCRI findings
- Integrate intel & activity reports into risk scoring



A Combat Support Agency

DISA Testing Success Stories

- **Implemented available SCM capabilities without impact to current operations and within current operating budget (Currently reporting on more than 21,000 DISA assets)**
- **Implemented lesson learned from Army Pilot Q4FY10-Q1FY11): Provide structured and controlled attribution to responsible organizations for action**

- **Discovered SIPRNet URLs configured on NIPRNet**
  - **Upon investigation, discovered they were for NIPRNet test systems simulating SIPRNet systems**
- **Discovered more than 200 DISANet hosts (out 4911) with DAT files older than 7 days.**
  - **62 dat files > 14 days**
  - **8 dat files > 100 days**
  - **2 dat file > 1 year**
- **Using ACCM, discovered an XP host that did not have Air Defense installed to prevent dual-homed wired and wireless connections**

DISA

A Combat Support Agency

QUESTIONS

http://www.disa.mil/scm

SCMPMO@DISA.MIL

NDAA

A Combat Support Agency

H. R. 6523—198

Subtitle D—Cyber Warfare, Cyber Security, and Related Matters

SEC. 931. CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY.

(a) IN GENERAL.—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

(2) The **automation of continuous monitoring** of the effectiveness of the **information security policies, procedures, and practices** within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices, **including automation of**—

(A) **management, operational, and technical controls of every information system** identified in the inventory required under section 3505(c) of title 44, United States Code; and

(B) management, operational, and technical controls relied on for evaluations under section 3545 of title 44, United States Code.

(b) DEFINITIONS.—In this section:

(1) The term ‘‘information security incident’’ means an occurrence that—

(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

(2) The term ‘‘information infrastructure’’ means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

(3) The term ‘‘national security system’’ has the meaning given that term in section 3542(b)(2) of title 44, United States Code.

Federal C&A Policy is Changing

A Combat Support Agency

NIST SP 800-37 Rev. 0

The previous version had 4 Steps

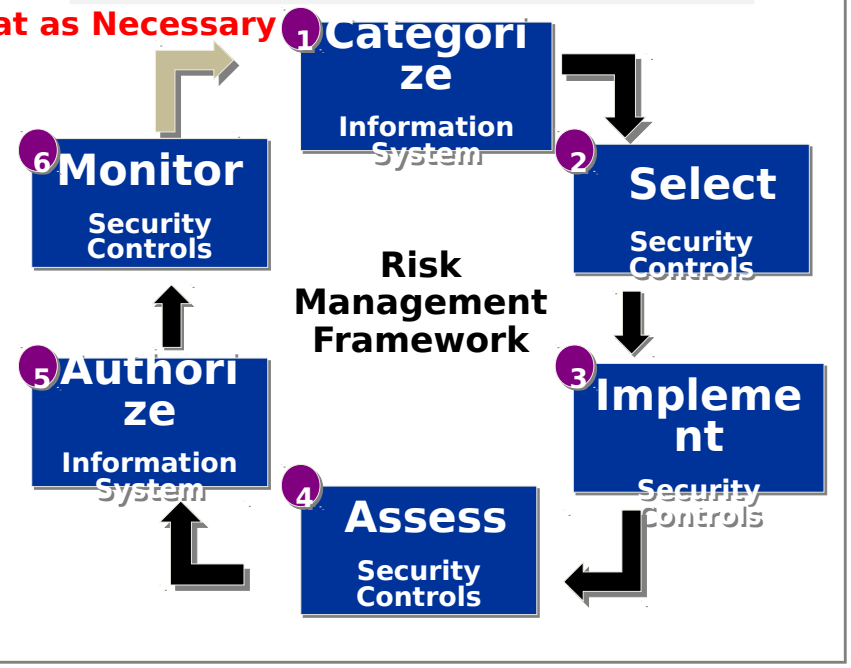
1. Initiation Phase
2. Security Certification Phase
3. Security Accreditation Phase
4. Continuous Monitoring Phase

- Preparation
- Notification and Resource Identification
- System Security Plan Analysis, Update and Acceptance
- Security Control Assessment
- Security Certification Documentation
- Security Accreditation Decision
- Security Accreditation Documentation
- Configuration Mgmt. and Control
- Security Control Monitoring
- Status Reporting and Documentation

Repeat as Necessary

NIST SP 800-37 Rev. 1

The recently released version has 6 steps



= *NIST 800-37 Rev. 1 Steps*

= *NIST 800-37 Rev. 0 Mapping to Rev. 1 Steps*

DISA
A Combat Support Agency

SCM Components

- **Antivirus/Antispyware** – Antivirus and Antispyware products for DoD
- **Asset Configuration Compliance Module (ACCM)** – HBSS module to perform system software inventory using SCAP Common Platform Enumerations (CPE)
- **Asset Data Service (ADS)** – Web application to collect bulk asset records and attributes from HBSS and other CC/S/A asset management systems.
- **Asset Publishing Service (APS)** – HBSS module to publish SCAP compliance data to the NCES JUM.
- **Assured Compliance Assessment Solution (ACAS)** – SCAP validated network vulnerability assessment tool.
- **Automatable STIG Publication** – VMS capability to publish SCAP STIGs (XCCDF/OVAL)
- **Continuous Monitoring and Risk Scoring (CMRS)** – Web services and applications to collect machine to machine SCAP data to present common risk scores and AOR/UNIT compliance scores. (e.g., Dept. of State iPOST)
- **Digital Policy Management Service (DPMS)** – Consolidated system to manage the creation, maintenance, and distribution of STIGs, IAVMs, SCAP content, Patches, HIPs signatures. Combining and merging partial capabilities of VMS, IAVM System, eSCAPE, Patch Service.
- **Enterprise Network Mapping and Leak Detection Solution (ENMLDS)** – Enterprise network mapping, host discovery, and domain leak detection.
- **Enterprise Mission Assurance Support Service (eMASS)** –DIACAP support web application
- **Gold Disk** – DoD GOTs product to perform Windows STIG/IAVM assessments and remediation

DISA
A Combat Support Agency

SCM Components (cont)

- **Host Based Security System (HBSS)** – RSD, PA, ePO Rollup, OAM
  - **RSD** – reports rogue, unmanaged hosts on ePO managed networks.
  - **Policy Auditor** – SCAP validated agent-based tool that assesses host security compliance
  - **ePO Rollup** – HBSS reporting capability that reports to the Tier 1
  - **OAM** – HBSS module to allow assignment of operational attributes to host records.
- **IAVM System** – Collaborative IAVM pre-coordination web site for CC/S/A to input information related to pending IAVM issuances.
- **Patch Management, WSUS** – Enterprise patch distribution web server and Windows patch service
- **Ports, Protocols, and Services (PPSM DB)** – Web application to track risk associated to well-known network ports, protocols, and services (PPS). Supports the registration and tracking of approved application PPS.
- **Remediation / Remediation Manager** – Potential follow on to SCRI. Pending the definition of enterprise requirements, the Remediation program may be a remediation policy manager to manage approved or recommended mitigations/remediation or a remediation tool to perform remediation/mitigations on hosts.
- **Secure Configuration Compliance Validation Initiative (SCCVI)** – Network vulnerability assessment tool.
- **Secure Configuration Remediation Initiative (SCRI)** – Enterprise patch and remediation tool.
- **Vulnerability Management System (VMS)** – Web application to track Operational Directive acknowledgement and compliance, IAVM compliance, and STIG compliance for technical and non-technical assets.

DEFENSE INFORMATION SYSTEMS AGENCY